

REMARKS

I. Introduction

In the August 29, 2006, Office Action in this application (hereinafter "Office Action"), the United States Patent and Trademark Office rejected Claims 19-29, 31-40, 42-45, and 47-49 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 19-29, 31-40, 42-45, and 47-49 are now amended to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Thus, the § 112 rejections are now moot and a withdrawal of the § 112 rejection with respect to those claims is requested. The Office Action also rejected Claims 1, 3, 5-7, 10, 12-19, 24-26, 30-37, 42-45, and 47-49 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,260,145, to Komura et al. (hereinafter "Komura"). Finally, Claims 2, 4, 8, 11, 20-23, 27-29, and 38-40 were rejected under 35 U.S.C. § 103(a) as unpatentable over Komura in view of U.S. Patent No. 6,715,073, to An et al. (hereinafter "An et al."). For the following reasons, applicant asserts that the claims of the present application are not anticipated or obvious over the cited and applied prior art, alone or in combination, because the prior art fails to teach or suggest a document processing server which encrypts and processes the document obtained from a sender, and provides the processed document to recipients through a secured communication channel as recited in the claims of the present invention. Prior to discussing more detailed reasons why applicant believes that the claims of the present application are allowable, a brief description of the present invention and the cited references are presented.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100

A. Summary of the Claimed Invention

In accordance with the present invention, a system and method for processing communications between a sender computing device and at least one recipient computing device utilizing a document processing server are provided. The document process server is a separate entity from the sender computing device and recipient computing devices. Initially, a sender establishes a secure communication with the *document processing server* and requests the processing of an electronic document, which can include the appending of a digital signature. The document processing server processes the electronic document and establishes secure communications with one or more designated recipients. Further, upon the sender's request, the document processing server implements sender-specified recipient identity verification and provides further processing of the electronic document as designated by the recipients. In this manner, the sender and the designated recipient do not have to exchange any encryption keys, including a private encryption key, since the sender and the recipient communicate only with the document processing server, not each other. The document processing server is responsible for any processing relating to identification and encryption/decryption of the document.

B. Summary of Komura (U.S. Patent No. 6,260,145)

Komura discloses a system and method for authenticating digital information. Initially, a server appends verification data to an electronic document to be circulated through terminal units for persons in charge. Each terminal unit is allocated a unique function in advance. The server sends the document with verification data appended to the first terminal unit in a predetermined route (a route for circulation). Each terminal unit sends the document directly to a next terminal unit in the predetermined route and **applies its unique function to the verification data in turn when receiving the document.** The last terminal unit in the predetermined route sends the document with verification data back to the server. Upon receipt of the electronic document that

has been circulated through the terminal units for persons in charge, the server examines the function-applied value appended to the document to determine whether the document has been circulated correctly through the persons in charge, or via the correct route. However, Komura fails to teach a server which is responsible for any processing relating to identification and encryption/decryption of the document.

C. Summary of An et al. (U.S. Patent No. 6,715,073)

An et al. discloses a system and method for *managing* the issuance, renewal, and revocation of *digital certificates* for Web browsers and servers using vault technology. Generally, the vault technology provides a secure environment in a web server using a vault controller for running a secure Web-based registration process and enabling secure application. The controller provides security from other processes running on the same server and secure areas, or personal storage vaults to which only the owner has a key. System operators, administrators, certificate authorities, registration authorities, and others cannot get to stored information or secure processes in such personal vaults. The system in An et al. includes registration and certification authorities, and a Web server (vault controller) maintaining personal storage vaults in the controller for users. Each personal vault runs programs on the controller under a unique UNIX user ID. This particular UNIX user ID is linked to a user with a specific vault access certificate. The content of the vault is encrypted and contains an encryption key pair and a signing key pair, both of which are password protected. Data storage provided by the controller is owned by the same user ID assigned to the vault. A registration authority running as a software application in the controller processes requests to issue, renew and revoke **digital certificates issued by a certification authority using two pairs of public-private keys.**

II. Examiner's Interview Summary

Applicant thanks the Examiner for taking time on December 1, 2006, to participate in a telephone interview. The interview was conducted in light of the Office Action rejecting Claims 1-3, 12-15, 17, 20-28, 32-36, and 38-65. Participating in the October 13, 2006, interview were the Examiner and applicant's representative, Sunah Lee. The discussion in the interview was directed to the distinction between the independent claims and the prior art, particularly the citations of Claims 1, 19, and 37. Applicant also thanks the Examiner for allowing a second telephone interview in future to expedite the process of the examination, in case any new art is applied.

III. Rejection of Claims Under 35 U.S.C. § 112

Claims 19-29, 31-40, 42-45, and 47-49 were rejected under 35 U.S.C. § 112, second paragraph, for failing to particularly point out and distinctly claim the subject matter regarded as the invention.

In regard to Claims 19, 20, 21, 25-29, 34, and 35, the recitation "operable" has been removed, as the Office Action suggested. In light of the above, applicants submit that Claims 19-29, 31-40, 42-45, and 47-49 are fully compliant with 35 U.S.C. § 112, second paragraph, and request that these rejections be withdrawn.

IV. Rejection of Claims 1, 3, 5-7, 10, 12-19, 24-26, 30-37, 42-45, and 47-49 Under 35 U.S.C. § 102

The Office Action rejected Claims 1, 3, 5-7, 10, 12-19, 24-26, 30-37, 42-45, and 47-49 under 35 U.S.C. § 102(b) as being anticipated by Komura. The Office Action asserts that Komura discloses each and every element of these claims. As described in more detail below, applicant respectfully disagrees.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

A. Claim 1

In its amended form, Claim 1 recites:

A method for a document processing server to process communications between a sender and at least one recipient and to verify an identity of the sender and the at least one recipient for establishing a secured communication channel, the method comprising:

at the document processing server:

obtaining the a request from the sender to transmit an electronic document to at least one recipient;

obtaining an electronic document corresponding to the request from the sender;

processing the electronic document wherein processing the electronic document includes encrypting the electronic document with an encryption key corresponding to at least one recipient;

verifying the identity of the designated at least one recipient and the identity of the sender;

upon verification, establishing a secured communication channel with the at least one recipient;

transmitting the processed electronic document to the designated at least one recipient;

wherein the sender and the designated at least one recipient do not verify the identity of each other; and

wherein the sender and the designated at least one recipient do not exchange encryption keys.

Claim 1 recites a method for a document processing server to process communications between a sender and at least one recipient and to verify an identity of the sender and the at least one recipient for establishing a secured communication channel to transmit a document. In particular, Claim 1 includes the limitations of "processing the electronic document, wherein processing the electronic document includes encrypting the electronic document with an

encryption key corresponding to the designated at least one recipient," which are done "at the document processing server."

Additionally, Claim 1 recites "verifying the identity of the designated at least one recipient and the identity of the sender" at the document processing server so that "the sender and the designated at least one recipient do not verify the identity of each other," or "the sender and the designated at least one recipient do not exchange encryption keys."

Simply stated, the method disclosed in Komura does not verify the identity of a recipient and the identity of a sender at a server in order to transmit an electronic document from the sender to the recipient. Instead, the sender and the recipient in Komura do verify the identity of each other upon an exchange of an electronic document.

In Komura, each terminal sends the document directly to a next terminal in the predetermined route and appends verification data, such as a digital signature, before sending the documents to the next terminal. Upon receipt of the document, "a signature verification unit" of a recipient terminal verifies the verification data appended to documents received from a sender terminal and, after verification, the recipient terminal applies its unique function to verification data.

For example, Col. 6, lines 44-50, of Komura disclose:

In procedure P3, the terminal 12 sends the document, the ID code, the function-applied value, and **the digital signature 1** from its interface 41 to the interface 51 of the terminal 13. Upon receipt of the information via the interface 51, **the signature verification unit 52 verifies the digital signature appended by the person in charge 1**. If the digital signature is verified as that appended by the person in charge 1, the function application unit 53 applies the function 2 stored in the function storage unit 55 to the received function-applied value. **The signature creating unit 54 then appends the digital signature 2 to the document**, the ID code, and the function-applied value "function 2 (function 1 (value))." (Emphasis added.)

As described in the above-cited passage, a sender terminal sends "the document, the ID code, the function-applied value, and **the digital signature**" to a recipient terminal. Subsequently, "the signature verification unit" in the recipient terminal verifies "the digital signature appended by the person in charge" of the sender terminal unit. For the reasons set forth above, Komura fails to teach "verifying the identity of the designated at least one recipient and the identity of the sender" at the document processing server so that "the sender and the designated at least one recipient do not verify the identity of each other."

Further, Komura also fails to teach "the sender and the designated at least one recipient do not exchange encryption keys," as recited in Claim 1. For example, Col. 5, lines 15-20, of Komura discloses:

An example of a way for the data recipient to verify the originator's identity is to decrypt the digital signature using a public key described in a certificate published by an authentication office, and verify its contents. The secret key used to create the digital signature and the public key described in the certificate are paired with each other, so that data encrypted by using **the secret key can be decrypted by using the public key**. (Emphasis added.)

The cited passage discloses that a secret key and a public key can be paired with each other to verify the originator's identity. One of ordinary skill in the art would understand that a public key in the public key encryption system serves the purpose of encrypting and decrypting a particular secret key that is **exchanged** between a sender and a recipient. Thus, the cited passage teaches an exchange of an encryption key (i.e., an encrypted secret key which is use to encrypt data) between a sender and a recipient. This is contrary to the above mentioned limitation recited in Claim 1. Applicant respectfully submits that Komura also fails to teach or suggest "the sender and the designated at least one recipient do not exchange encryption keys" where neither the sender nor the recipient is the document processing server.

For the reasons set forth above, applicant respectfully submits that Komura fails to expressly or inherently teach, disclose, or suggest each and every element of Claim 1. Specifically, as explained above, Komura fails to disclose or suggest "verifying the identity of the designated at least one recipient and the identity of the sender" at the document processing server so that "the sender and the designated at least one recipient do not verify the identity of each other," or "the sender and the designated at least one recipient do not exchange encryption keys." Accordingly, for this reason, applicant respectfully submits that amended Claim 1 is allowable and requests that the rejection be withdrawn.

B. Claims 3, 5-7, 10, 12-18, and 47

Claims 3, 5-7, 10, 12-18, and 47 are dependent on Claim 1. For the above mentioned reasons with regard to Claim 1, applicant respectfully suggests that the cited reference fails to teach each of the elements recited in the dependent claims. Accordingly, applicant respectfully requests withdrawal of the § 102 rejection with regard to dependent Claims 3, 5-7, 10, 12-18, and 47.

C. Claim 19

Claim 19 recites:

A system for processing communications, the system comprising:

- a sender computing device operable to transmit a request to process an electronic document;
- at least one recipient computing device corresponding to an identifiable communication channel; and
- a document processing server, the document processing server operable to establish secure communications with the sender computing device and the at least one recipient computing device;

wherein the document processing server processes an electronic document and transmits the processed electronic document between the sender computing device and the recipient computing device without the sender computing device and the at least one recipient computing device exchanging encryption keys.

Applicant respectfully submits that Komura fails to teach or suggest each and every limitation recited in Claim 19. For example, Komura fails to teach "a document processing server operable to verify the identities of the sender and the at least one recipient" so that "the sender and the at least one recipient do not verify the identity of each other," as recited in Claim 19. Simply stated, Komura discloses a server computing device (server) that is patentably distinguishable over a document processing server as recited in Claim 19. While the document processing server in the claimed invention verifies a sender and the designated recipients so that the document processing server can receive a document from the sender and then securely transmit the document to each of the designated recipients, the server in Komura does not verify each of the designated recipients or transmit the document to each of the designated recipients. Instead, each terminal unit in Komura verifies the verification data upon receipt of the document, applies its unique function, appends a digital signature, and sends the document to a next terminal unit. For those reasons stated above, Komura fails to teach each and every limitation recited in Claim 19. Applicant respectfully requests withdrawal of the § 102 rejection with respect to Claim 19.

D. Claims 24-26, 30-36, and 48

Claims 24-26, 30-36, and 48 are dependent on Claim 19. As discussed above, Komura fails to teach or suggest each of the limitations recited in Claim 19. For the above mentioned reasons with regard to Claim 19, applicant respectfully asserts that the cited reference fails to teach each of the elements recited in the dependent claims. Accordingly, applicant respectfully requests withdrawal of the § 102 rejection with regard to dependent Claims 24-26, 30-36, and 48.

E. Claim 37

For similar reasoning with respect to Claims 1 and 19, applicant asserts that Komura does not teach "a document processing component configured to verify the identity of the one of the

plurality of recipient computing devices and the sender computing device and to process document requests from the sender computing device" so that "the sender computing device does not verify the identity of the each of the plurality of recipient computing devices" and "the each of the plurality of recipient computing devices does not verify the identity of sender computing device," as recited in Claim 37. As described above, a server disclosed in Komura does not "verify the identity of the one of the plurality of recipient computing devices and the sender computing device" but each computing device has to verify each other for a secure communication. Accordingly, Komura fails to teach each and every limitation recited in Claim 37. Applicant respectfully requests withdrawal of the § 102 rejection with respect to Claim 37.

F. Claims 41-45 and 49

Claims 41-45 and 49 are dependent on Claim 37. As discussed above, Komura fails to teach or suggest each of the limitations recited in Claim 37. For the above-mentioned reasons with regard to Claim 37, applicant respectfully asserts that the cited reference fails to teach each of the elements recited in the dependent claims. Accordingly, applicant respectfully requests withdrawal of the § 102 rejection with regard to dependent Claims 41-45 and 49.

V. Rejection of Claims 2, 4, 8, 11, 20-23, 27-29, and 38-40 Under 35 U.S.C. § 103

The Office Action rejected Claims 2, 4, 8, 11, 20-23, 27-29, and 38-40 under 35 U.S.C. § 103(a) as being unpatentable over Komura in view of An et al. The Office Action asserts that Komura and An et al. suggest each and every element of these claims and that it would be obvious to combine the teachings of Komura and An et al. Applicant respectfully disagrees.

As described above, a primary reference, Komura, fails to teach, or suggest all the limitations of Claims 1, 19, and 37. However, An et al. does not make up the defects of Komura

since An et al. merely teaches a system and method for managing the issuance, renewal, and revocation of digital certificates for Web browsers and servers using vault technology.

The system in An et al. includes a Web server (vault controller) having personal storage vaults in the controller for users, and registration and certification authorities. Each personal vault runs programs on the controller under a unique UNIX user ID. This particular UNIX user ID is linked to a user with a specific vault access certificate (digital certificate). The content of the vault is encrypted and contains an encryption key pair and a signing key pair, both of which are password protected. A registration authority running as a software application in the controller processes requests to issue, renew, and revoke digital certificates issued by a certification authority using two pairs of public-private keys. In sum, An et al. is concerned with digital certificates to determine whether the Web browsers and servers should be authorized to access secure applications.

However, the method disclosed in An et al. has nothing to do with "verifying the identity of the designated at least one recipient and the identity of the sender" at the document processing server so that "the sender and the designated at least one recipient do not verify the identity of each other," or "the sender and the designated at least one recipient do not exchange encryption keys," as recited in Claim 1. Similarly, the system disclosed in An et al. has nothing to do with "a document processing server" or "a document processing component" which is configured to verify the identities of a sender and recipients, as recited in Claims 19 and 37. As set forth above, the defects of Komura cannot be cured by An et al. Under § 103, a *prima facie* case of obviousness is established only if the cited references, alone or in combination, teach each of the limitations of the recited claims. *In re Bell*, 991 F.2d 781 (Fed. Cir. 1993). For these reasons, Komura and An et al., alone or in combination, fail to disclose or suggest each limitation recited in Claims 1, 19, and 37. Claims 2, 4, 8, and 11 depend from Claim 1. Claims 20-23 and 27-29


depend from Claim 19. Claims 38-40 depend from Claim 37. Claims 2, 4, 8, 11, 20-23, 27-29, and 38-40 also include a myriad of recitations not disclosed, taught, or suggested by any of the cited and applied references, particularly when the recitations are considered in combination with the recitations of claims from which these claims depends. Accordingly, applicant respectfully requests a withdrawal of the § 103 rejection with respect to Claims 2, 4, 8, 11, 20-23, 27-29, and 38-40.

VI. Conclusion

In view of the foregoing remarks, applicant submits that all pending claims are in patentable condition and respectfully requests an early notice to that effect. The Examiner is requested to contact applicant's attorney at the number provided below should any questions or issues remain.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS^{PLLC}



for Mauricio

Mauricio A. Uribe
Registration No. 46,206
Direct Dial No. 206.695.1728

sunah lee
No. 53,198

MAU\SKL:lal

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100